THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

SYLVIA TILLMAN, AMRESH JAIJEE, VIVIAN YATES, RICHARD GAMEN, CHERYL GAMEN, on behalf of themselves and all others similarly situated, Plaintiffs, vs. MORGAN STANLEY SMITH BARNEY, LLC, Defendant.	Case No.: _____ **CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

Plaintiffs Sylvia Tillman, Amresh Jaiejee, Vivian Yates, Richard Gamen, and Cheryl Gamen ("Plaintiffs") bring this Class Action Complaint against Morgan Stanley Smith Barney, LLC ("Morgan Stanley" or "Defendant"), as individuals and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiffs bring this class action against Morgan Stanley for its failure to properly secure and safeguard personal identifiable information, including without limitation, names, Social Security numbers, passport numbers, addresses, telephone numbers, email addresses, account numbers, dates of birth, income, asset value and holding information (collectively, "personal identifiable information" or "PII"). Plaintiffs also allege Defendant failed to provide timely, accurate, and adequate notice to Plaintiffs and similarly situated Morgan Stanley current and former customers ("Class Members") that their PII had been lost and precisely what types of information was unencrypted and in the possession of unknown third parties.

2. Morgan Stanley sells securities and other financial products with offices nationwide. When individuals sign up for a Morgan Stanley account, they are required to give the firm an extensive amount of PII for themselves and others associated with the account. Morgan Stanley retains this information on computer hardware—even after a customer closes an account—and promises the public it will protect "the confidentiality and security of client information" by, among other things, using "computer safeguards and secured files and buildings."

3. This case does not involve a breach of a computer system by a third party, but rather an unauthorized disclosure of the PII of Plaintiffs and the class by Defendant to unknown third parties.

4. On or about July 9, 2020, Morgan Stanley began notifying various state Attorneys General about multiple data breaches that occurred as early as 2016. Around the same time, Defendant mailed a *Notice of Data Breach* to current and former customers affected by the breaches. First, in 2016, Morgan Stanley closed two data centers and decommissioned the computer equipment. Morgan Stanley hired a vendor to remove customers' data from the equipment. Subsequently, Morgan Stanly learned that the data was not fully "wiped" clean, and admits that "certain devices believed to have been wiped of all information still contained some unencrypted data." Now, according to Defendant, that equipment is missing.

5. Second, in 2019, Morgan Stanley disconnected and replaced multiple computer servers in various branch locations. The old servers, which still contained customers' data, were thought to be encrypted, but Morgan Stanly subsequently learned that a "software flaw" on the servers left "previously deleted data" on the hard drives "in an unencrypted form." Now those servers are also missing (the 2016 and 2019 incidents will be collectively referred to herein as the "Data Breach").

6. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and the Class Members' PII, Defendant assumed legal and equitable duties to those individuals. Defendant admits that the unencrypted PII that has "left [its] possession" included PII from the account holders and any "individual(s) associated with your account(s), including account names and numbers (at Morgan Stanley and any linked bank accounts), Social Security number, passport number, contact information, date of birth, asset value and holdings data."

7. The missing equipment and servers contain everything unauthorized third-parties need to illegally use Morgan Stanley's current and former customers' PII to steal their identities and to make fraudulent purchases, among other things.

8. Not only can unauthorized third-parties access Defendant's customers' PII, the PII can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. Plaintiffs and Morgan Stanley's current and former customers face a lifetime risk of identity theft, which is heightened here by the loss of customers' Social Security number.

9. This PII was compromised due to Morgan Stanley's negligent and/or careless acts and omissions and the failure to protect customers' data. In addition to Morgan Stanley's failure to prevent the Data Breach, Defendant failed to detect the Data Breach for years, and when they did discover the Data Breach, it took them over a year, possibly longer, to report it to the affected individuals and the states' Attorneys General.

10. As a result of this delayed response, Plaintiffs and Class Members had no idea their PII had been compromised, and that they were, and continue to be, at significant risk to identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

11. Plaintiffs bring this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect its customers' PII; (ii) warn customers of its inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates several California statutes.

12. Plaintiffs and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, (iv) deprivation of rights they possess under the California Unfair Competition Law, (Cal. Business & Professions Code § 17200, *et seq*.); and (v) the continued and certainly an increased risk to their PII, which: (a) remains unencrypted and available on the missing equipment for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

13. Morgan Stanley disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that its customers' PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As the result, the PII of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiffs and Class Members have a continuing

interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

14. Plaintiff Sylvia Tillman is a Citizen of California residing in San Diego County, California. In the early or mid-1990s, Ms. Tillman signed up for a California Uniform Transfers to Minors Act ("UTMA/CA") account for her minor daughter through Morgan Stanley in California. A UTMA/CA account allows an appointed custodian to manage the minor's account until the latter turns 18. Ms. Tillman closed the UTMA/CA account in or about 2000. Ms. Tillman received Morgan Stanley's *Notice of Data Breach,* dated July 11, 2020, on or about that date. The notice specifically stated that her information associated with her UTMA/CA account was subject to the Data Breach.

15. Plaintiff Amresh Jaijee is a citizen of New York residing in New York City. Ms. Jaijee opened her 401K individual retirement account at a Morgan Stanley office in New York in or about 2012. The account is still active. Ms. Jaijee received Morgan Stanley's *Notice of Data Breach*, dated July 10, 2020, on or about that date.

16. Plaintiff Vivian Yates is a citizen of Florida residing in Riverview, Florida. Ms. Yates signed up for her 529 college savings plan account at the Morgan Stanley office located in Florida, in or about 2015. Ms. Yates received Morgan Stanley's Notice of Data Breach, dated July 10, 2020, on or about that date.

17. Plaintiffs Richard Gamen and Cheryl Gamen, a married couple, are citizens of Illinois and reside in New Lenox, Illinois. In or about 1989, Richard Gamen and Cheryl Gamen signed up for a brokerage account through Morgan Stanley's office in Chicago, Illinois. In addition, Ms. Gamen, rolled over her 401K individual retirement account to Morgan Stanley, and

both accounts were closed years ago. The Gamens received Morgan Stanley's Notice of Data Breach, both dated July 11, 2020, on or about that date.

18. Defendant Morgan Stanley Smith Barney, LLC is a limited liability company organized under the laws of Delaware, with its principal place of business headquartered at 1585 Broadway, New York, NY 10036.

19. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiffs. Plaintiffs will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

20. All of Plaintiffs' claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

21. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant. Plaintiffs are citizens of California, Florida, New York, and Illinois and therefore diverse from Defendant, which is headquartered in New York.

IV. FACTUAL ALLEGATIONS

Background

22. Morgan Stanley is a multinational investment bank and financial services company with offices in over 40 countries with more than 60,000 employees. The firm's clients include corporations, governments, institutions, and individuals. Morgan Stanley ranked No. 62 in the

2019 Fortune 500 list of the largest United States corporations by total revenue.

23. Plaintiffs and the Class Members, as current and former customers, relied on this sophisticated Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Customers demand security to safeguard their PII.

24. Defendant had a duty to adopt reasonable measures to protect Plaintiffs' and Class Members' PII from involuntary disclosure to third parties. Morgan Stanley touts the secure nature of its system in its "Privacy Pledge":

> Morgan Stanley's long-standing commitment to safeguard the privacy of information our clients entrust to us is essential to our goal to be the world's first choice for financial services. **Protecting the confidentiality and security of client information has always been an integral part of how we conduct our business** worldwide.
>
> We pledge to continue to ensure that our global business practices protect your privacy. (emphasis added)[1]

25. Morgan Stanley also claims that the firm "use[s] personal information . . . to detect security incidents and protect against malicious, deceptive, fraudulent, or illegal activity."[2] The company further claims:

> To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. We have policies governing the proper handling of customer information by personnel and requiring third parties that provide support to adhere to appropriate security standards with

[1] Morgan Stanley's *Privacy Pledge*, *available at*: https://www.morganstanley.com/privacy-pledge (last visited July 22, 2020).
[2] Morgan Stanley's *U.S. Privacy Policy and Notice*, *available at*: https://www.morganstanley.com/disclaimers/us-privacy-policy-and-notice.html (last visited July 22, 2020).

respect to such information.[3]

26. Morgan Stanley collects and maintains PII from its individual account holders, including but not limited to: "Social Security number and income;" "investment experience and risk tolerance;" and "checking account number and wire transfer instructions."[4]

27. Individual Morgan Stanley account holders may also supply the firm with personal identification (including passport numbers), mailing and billing addresses, telephone numbers, emails addresses, dates of birth, bank account numbers, and specific asset value and holdings information.

The Data Breach

28. Beginning on or about July 9, 2020, Morgan Stanley sent customers a *Notice of Data Breach*.[5] Morgan Stanley, identifying itself as "Morgan Stanley Smith Barney LLC. Member SIPC. / Morgan Stanley Private Bank, National Association. Member FDIC," informed the recipients of the notice that:

> In 2016, Morgan Stanley closed two data centers and decommissioned the computer equipment that processed client information in both locations. As is customary, we contracted with a vendor to remove the data from the devices. We subsequently learned that certain devices believed to have been wiped of all information still contained some unencrypted data. We have worked with outside technical experts to understand the facts and any potential risks [(the "Data Center Event")].[6]

29. On or about July 10, 2020, Morgan Stanley sent data breach notifications to various state Attorneys General, including Iowa's Attorney General Tom Miller, signed by Gerard Brady,

---

[3] Morgan Stanley's *U.S. Customer Privacy Notice*, *available at*: https://www.morganstanley.com/disclaimers/im-customer-privacy-notice.pdf (last visited July 22, 2020).
[4] *Id.*
[5] *See Notice of Data Breach*, filed July 10, 2020 with the California Attorney General, a true and correct copy of which is attached hereto as Exhibit 1 ("Ex. 1").
[6] Ex. 1, p.1.

Morgan Stanley's Chief Information Security Officer. Brady reported the 2016 incident above and added information about another related breach that began in 2019:

> Separately, in 2019, Morgan Stanley disconnected and replaced certain computer servers (the "WAAS device") in local branch offices. Those servers had stored information on encrypted disks that may have included personal information. During a recent inventory, we were unable to locate a small number of those devices. The manufacturer subsequently informed us of a software flaw that could have resulted in small amounts of previously deleted data remaining on the disks in unencrypted form. We have worked with outside technical experts to understand the facts and any potential risks (the "WAAS Device Event").[7]

30. Morgan Stanley admitted in the *Notice of Data Breach* and the letters to the Attorneys General that the hardware involved in both the 2016 Data Center Event and the 2019 WAAS Device Event "left our possession" at some point containing unencrypted information, and "it is possible that data associated with your account(s) could have remained on some of the devices when they left our possession."[8]

31. Defendant further admitted that the unencrypted PII that left its "possession" included information from the account holder and any "individual(s) associated with your account(s), including account names and numbers (at Morgan Stanley and any linked bank accounts), Social Security number, passport number, contact information, date of birth, asset value and holdings data."[9]

32. For an UTMA/CA account, for example, the lost PII would include PII belonging to the UTMA/CA custodian managing the account and the minor account holder.

33. In response to the Data Breach, Morgan Stanley claims it has "instituted enhanced

[7] *See Letter from Morgan Stanley's Gerard Brady to Iowa's Attorney General Tom Miller*, dated July 10, 2020, a true and correct copy of which is attached hereto as Exhibit 2 ("Ex. 2").
[8] Ex. 2.
[9] Exs. 1, 2.

security procedures on your account(s), including continuous fraud monitoring and monitoring of information about malicious online activity and evidence of misuse of any Morgan Stanley data." It has also "taken steps to further strengthen controls aimed at reducing the risk that such an incident could occur in the future." [10]

34. The equipment containing Plaintiffs' and Class Members' unencrypted information is missing, and is or may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII for targeted marketing without the affected customers' approval. Unauthorized individuals can easily access Morgan Stanley's customers' unencrypted, unredacted information from these multiple devices, including Social Security numbers, passport numbers, addresses, telephone numbers, email addresses, checking account numbers, dates of birth, income, asset value and holding information.

35. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for current and former customers, causing Plaintiffs' and Class Members' PII to be exposed.

Securing PII and Preventing Breaches

36. Defendant could have prevented this Data Breach by properly encrypting the lost equipment and computer files containing PII on those lost hard drives. And, as Defendant claims it does, properly securing the "building" or location housing the equipment. Or Morgan Stanley could have destroyed the data, especially decadeold data from former customers like Plaintiff Tillman.

37. Defendant's negligence in safeguarding its customers' PII is exacerbated by the repeated warnings and alerts directed to protecting and securing electronics. And Morgan Stanley,

[10] Exs. 1, 2.

specifically, has suffered breaches that involved stolen equipment containing customer PII only two years before this Data Breach.[11]

38. Defendant has acknowledged the sensitive and confidential nature of the PII. To be sure, collection, maintaining, and protecting PII is vital to many of Defendant's business purposes. Defendant has acknowledged through conduct and statements that the misuse or inadvertent disclosure of PII can pose major privacy and financial risks to impacted individuals, and that under state law they may not disclose and must take reasonable steps to protect PII from improper release or disclosure. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite their own acknowledgment of its duties to keep PII private and secure, Defendant failed to take appropriate steps to protect the PII of Plaintiffs and the proposed Class from being compromised.

39. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[12] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[13]

40. The ramifications of Defendant's failure to keep its customers PII secure are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that

[11] Aruna Viswanatha, *Morgan Stanley Fined $1 Million for Client Data Breach*, The Wall Street Journal (2016), *available at*: https://www.wsj.com/articles/morgan-stanley-fined-1-million-for-client-data-breach-1465415374 (last visited July 24, 2020).
[12] 17 C.F.R. § 248.201 (2013).
[13] *Id.*

information and damage to victims may continue for years.

Value of Personal Identifiable Information

41. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[14] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[15] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[16]

42. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[17]

---

[14] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed July 24, 2020).

[15] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed July 24, 2020).

[16] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed July 24,, 2020).

[17] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited July 23, 2020).

43. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

44. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[18]

45. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security number, passport number, name, date of birth, address, and asset holdings and other financial information.

46. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[19]

---

[18] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited July 23, 2020).

[19] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited July 23, 2020).

47. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

48. The fraudulent activity resulting from the Data Disclosure may not come to light for years.

49. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[20]

50. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding its current and former customers' PII, including Social Security numbers and dates of birth, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Defendant's customers as a result of a breach.

51. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

52. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's decommissioned equipment, amounting to potentially millions of individuals' detailed, personal, finance-related information and thus, the significant

[20] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf (last visited July 24, 2020).

number of individuals who would be harmed by the loss of decommissioned equipment containing unencrypted data.

53. To date, Defendant has offered its customers only two years of credit monitoring service through a single credit bureau, Experian. The offered service is inadequate to protect Plaintiffs and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

54. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for its current and former customers' PII.

Plaintiff Tillman's Experience

55. In the early or mid-1990s, Plaintiff Sylvia Tillman signed up for a California Uniform Transfers to Minors Act ("UTMA/CA") account for her minor daughter through Morgan Stanley in California.

56. Ms. Tillman supplied Morgan Stanley with her and her daughters' personal identifiable information, including but not limited to her address and Social Security number. Ms. Tillman closed the UTMA/CA account in or about 1999.

57. Ms. Tillman received the *Notice of Data Breach*, dated July 11, 2020, on or about that date. It was addressed to "Sylvia Tillman cust[odian] for [her minor daughter] UTMA/CA."

58. As a result of the Data Breach notice, Ms. Tillman spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the *Notice of Data Breach*, communicating with Morgan Stanley representatives on the toll-free number supplied in the notice, exploring credit monitoring and identity theft insurance options, and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

59. Ms. Tillman is very careful about sharing her PII, and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

60. Ms. Tillman stores any and all documents containing her PII in a safe and secure digital location, and destroys any documents she receives in the mail that contain any of her PII, or that may contain any information that could otherwise be used to compromise her credit card accounts and identity. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

61. Ms. Tillman suffered actual injury and damages in paying money to Defendant for facilitating the UTMA/CA account before the Data Breach; expenditures which she would not have made had Defendant disclosed that it lacked data security practices adequate to safeguard customers' PII.

62. Ms. Tillman suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property that Ms. Tillman entrusted to Defendant for the purpose of facilitating the UTMA/CA account, which was compromised in and as a result of the Data Breach.

63. Ms. Tillman suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

64. Ms. Tillman has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially her and her daughters' Social Security numbers, being placed in the hands of unauthorized third-parties and possibly criminals.

65. Ms. Tillman has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded

from future breaches.

Plaintiff Jaijee's Experience

66. In or about 2012, Plaintiff Amresh Jaijee rolled over her 401K individual retirement account ("IRA") to Morgan Stanley at one of Defendant's offices in New York City.

67. Ms. Jaijee supplied Morgan Stanley with her personal identifiable information, including but not limited to her name, address, Social Security number, personal identification, checking account number and other financial information. She listed beneficiaries to her account and included their contact information. Ms. Jaijee's Morgan Stanley account is still active.

68. Ms. Jaijee received the *Notice of Data Breach*, dated July 10, 2020, on or about that date. It specifically states that in addition to her Social Security number, information about "any linked bank accounts" was breached as well.

69. As a result of the Data Breach notice, Ms. Jaijee spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the *Notice of Data Breach*, communicating with representatives of her bank that is linked to the Morgan Stanley IRA, checking her credit monitoring, exploring further credit monitoring and identity theft insurance options, and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

70. Ms. Jaijee is very careful about sharing her PII, and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

71. Ms. Jaijee stores any and all documents containing her PII in a safe and secure digital location, and destroys any documents she receives in the mail that contain her Social Security number or any other vital PII. Moreover, she diligently chooses unique usernames and passwords for her various online accounts, and routinely changes those passwords..

72. Ms. Jaijee suffered actual injury and damages in paying annual fees to Defendant for facilitating her 401K IRA account before the Data Breach; expenditures which she would not have made had Defendant disclosed that it lacked data security practices adequate to safeguard customers' PII.

73. Ms. Jaijee suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property that Ms. Jaijee entrusted to Defendant for the purpose of facilitating ther 401K IRA account, which was compromised in and as a result of the Data Breach.

74. Ms. Jaijee suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy, especially her Social Security number. Ms. Jaijee was recently contacted by an unidentified party by telephone that had her Social Security number and asked her to verify it. With the new information that her Social Security number has been lost by Defendant, this concerns her even more.

75. Ms. Jaijee has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially her Social Security number being placed in the hands of unauthorized third-parties and possibly criminals.

76. Ms. Jaijee has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiffs Richard Gamen's and Cheryl Gamen's Experiences

77. In or about 1989, Plaintiffs Richard Gamen and his wife, Cheryl Gamen, signed up for a brokerage account through Morgan Stanley's office in Chicago, Illinois.

The Gamens supplied Morgan Stanley with their personal identifiable information, including but not limited to their names, address and Social Security numbers. The brokerage account was terminated in or about 2010.

78. Ms. Gamen, in the early 1990's, rolled over her 401K individual retirement account to Morgan Stanley. That account was terminated in or about 2001.

79. Mr. and Ms. Gamen received a joint *Notice of Data Breach*, dated July 11, 2020, on or about that date, for the brokerage account. Ms. Gamen received another *Notice of Data Breach*, dated July 11, 2020, on or about that date, for her IRA account.

80. As a result of the Data Breach notices, Mr. Gamen spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the *Notice of Data Breach*, communicating with Morgan Stanley representatives on the toll-free number supplied in the notice, exploring credit monitoring and identity theft insurance options, and self-monitoring their accounts. Mr. Gamen also filed an online complaint with the Federal Trade Commission regarding this Data Breach. This time has been lost forever and cannot be recaptured.

81. Mr. and Ms. Gamen are very careful about sharing their PII, and have never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

82. Mr. Gamen stores any and all documents containing their PII in a safe and secure digital location, and destroys any documents they receive in the mail that contain any of their PII, or that may contain any information that could otherwise be used to compromise their credit card accounts and identities. Moreover, they diligently choose unique usernames and passwords for their various online accounts.

83. Mr. and Ms. Gamen suffered actual injury and damages in paying money to Defendant for facilitating their accounts before the Data Breach; expenditures which they would

not have made had Defendant disclosed that it lacked data security practices adequate to safeguard customers' PII.

84. The Gamens suffered actual injury in the form of damages to and diminution in the value of their PII—a form of intangible property that the Gamens entrusted to Defendant for the purpose of facilitating their accounts, which was compromised in and as a result of the Data Breach.

85. Mr. and Ms. Gamen suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and have anxiety and increased concerns for the loss of their privacy.

86. Mr. and Ms. Gamen have suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their lost PII, especially their Social Security numbers being placed in the hands of unauthorized third-parties and possibly criminals.

87. The Gamens have a continuing interest in ensuring that their PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Vivian Yates' Experiences

88. Vivian Yates signed up for her 529 college savings plan account at a Morgan Stanley office located in Florida, in or about 2015. Ms. Yates supplied Morgan Stanley with her personal identifiable information, including but not limited to her name, address, Social Security number, and other financial information. Ms. Yates received Morgan Stanley's Notice of Data Breach, dated July 10, 2020, on or about that date.

89. As a result of the Data Breach notice, Ms. Yates spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the *Notice*

of Data Breach, communicating with Morgan Stanley representatives on the toll-free number supplied in the notice, exploring credit monitoring and identity theft insurance options, and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

90. Ms. Yates is very careful about sharing her PII, and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

91. Ms. Yates stores any and all documents containing her PII in a safe and secure digital location, and destroys any documents she receives in the mail that contain any of her PII, or that may contain any information that could otherwise be used to compromise her credit card accounts and identities. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

92. Ms. Yates suffered actual injury and damages in paying money to Defendant for facilitating her accounts before the Data Breach; expenditures which she would not have made had Defendant disclosed that it lacked data security practices adequate to safeguard customers' PII.

93. Ms. Yates suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property that she entrusted to Defendant for the purpose of facilitating her accounts, which was compromised in and as a result of the Data Breach.

94. Ms. Yates suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of their privacy.

95. Ms. Yates has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her lost PII, especially her Social Security number being placed in the hands of unauthorized third-parties and possibly criminals.

96. Ms. Yates has a continuing interest in ensuring that her PII, which, upon

information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

97. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

98. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

> All individuals whose PII was compromised in the data breach first announced by Morgan Stanley on or about July 9, 2020 (the "Nationwide Class").

99. The California Subclass is initially defined as follows:

> All persons residing in California whose PII was compromised in the data breach first announced by Morgan Stanley on or about July 9, 2020 (the "California Subclass").

100. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, current or former employees, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

101. Plaintiffs reserve the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

102. Numerosity, Fed R. Civ. P. 23(a)(1): The Nationwide Class and California Subclass (the "Classes") are so numerous that joinder of all members is impracticable. Defendant has

identified thousands of customers whose PII may have been improperly accessed in the Data Breach, and the Classes are apparently identifiable within Defendant's records.

103. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiffs and Class Members;

b. Whether Defendant had respective duties not to disclose the PII of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendant had respective duties not to use the PII of Plaintiffs and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the PII of Plaintiffs and Class Members;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their PII had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class Members;

k. Whether Plaintiffs and Class Members are entitled to actual, damages, statutory damages, and/or punitive damages as a result of Defendant's wrongful conduct;

l. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct;

m. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach; and,

n. Whether Defendant violated the California Unfair Competition Law (Business & Professions Code § 17200, *et seq.*).

104. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendant's misfeasance.

105. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members, and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

106. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seek no relief that

is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex consumer class action litigation, and Plaintiffs intend to prosecute this action vigorously.

107. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

108. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be

unnecessary and duplicative of this litigation.

109. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

110. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

111. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

112. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

113. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiffs and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately, and accurately informed Plaintiffs and Class Members that their PII had been compromised;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class Members; and,

i. Whether Class Members are entitled to actual damages, statutory damages, injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

COUNT I
Negligence
(On Behalf of Plaintiffs and the Nationwide Class)

114. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 113.

115. As a condition of their using the services of Defendant, customers were obligated to provide Defendant with certain PII, including their date of birth, mailing addresses, Social Security numbers, passport numbers and personal financial information.

116. Plaintiffs and the Class Members entrusted their PII to Defendant on the premise

and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

117. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and Class Members could and would suffer if the PII were wrongfully disclosed.

118. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of their customers' PII involved an unreasonable risk of harm to Plaintiffs and Class Members, even if the harm occurred through the criminal acts of a third party.

119. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that Plaintiffs' and Class Members' information in Defendant's possession was adequately secured and protected.

120. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiffs' and Class Members' PII.

121. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class Members was reasonably foreseeable, particularly in light of Defendant's inadequate security practices and previous breach incidents involving Morgan Stanley customers' PII on stolen equipment.

122. Plaintiffs and the Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew of should have known of the inherent risks in collecting and storing the PII of Plaintiffs and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on

Defendant's systems.

123. Defendant's own conduct created a foreseeable risk of harm to Plaintiffs and Class Members. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of Plaintiffs' and Class Members' PII, including basic encryption techniques freely available to Defendant.

124. Plaintiffs and the Class Members had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

125. Defendant was in a position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

126. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiffs and Class Members within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

127. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiffs and Class Members.

128. Defendant has admitted that the PII of Plaintiffs and Class Members was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

129. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiffs and Class Members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiffs and Class Members during the time the PII was within Defendant's possession or control.

130. Defendant improperly and inadequately safeguarded the PII of Plaintiffs and Class Members in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

131. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect customers' PII in the face of increased risk of theft.

132. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of its customers' PII.

133. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiffs and Class Members the existence and scope of the Data Breach.

134. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and Class Members, the PII of Plaintiffs and Class Members would not have been compromised.

135. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiffs and Class Members and the harm suffered or risk of imminent harm suffered by Plaintiffs and the Class. Plaintiffs' and Class Members' PII was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

136. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity

costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of customers in their continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (ix) the diminished value of Defendant's goods and services they received.

137. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT II
Invasion of Privacy
(On Behalf of Plaintiffs and the Nationwide Class)

138. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 113.

139. Plaintiffs and Class Members had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

140. Defendant owed a duty to its customers, including Plaintiffs and Class Members, to keep their PII contained as a part thereof, confidential.

141. Defendant failed to protect and released to unknown and unauthorized third parties the PII of Plaintiffs and Class Members.

142. Defendant allowed unauthorized and unknown third parties access to and examination of the PII of Plaintiffs and Class Members, by way of Defendant's failure to protect the PII.

143. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiffs and Class Members is highly offensive to a reasonable person.

144. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs and Class Members disclosed their PII to Defendant as part of its use of Defendant's services, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiffs and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

145. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiffs and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

146. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

147. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiffs and Class Members.

148. As a proximate result of the above acts and omissions of Defendant, the PII of

Plaintiffs and Class Members was disclosed to third parties without authorization, causing Plaintiffs and Class Members to suffer damages.

149. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members in that the PII maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiffs and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and the Class.

COUNT III
Negligence Per Se
(On Behalf of Plaintiffs and the Nationwide Class)

150. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 113.

151. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant's, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

152. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of the Data Breach for companies of Defendant's magnitude, including, specifically, the immense damages that would result to Plaintiffs and Class Members due to the valuable nature of the PII at issue in this case—including social security numbers.

153. Defendant's violations of Section 5 of the FTC Act constitute negligence *per se*.

154. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

155. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class Members.

156. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of customers and former customers in its continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (ix) the diminished value of Defendant's goods and services they received.

157. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm,

including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiffs and the Nationwide Class)

158. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 113.

159. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and provided Defendant with their PII. In exchange, Plaintiffs and Class Members should have received from Defendant the goods and services that were the subject of the transaction and should have been entitled to have Defendant protect their PII with adequate data security.

160. Defendant knew that Plaintiffs and Class Members conferred a benefit on Defendant and accepted and have accepted or retained that benefit. Defendant profited from the purchases and used the PII of Plaintiffs and Class Members for business purposes.

161. The amounts Plaintiffs and Class Members paid for Defendant's goods and services should have been used, in part, to pay for the administrative costs of data management and security, including the proper and safe disposal of Plaintiffs' and Class Members' PII.

162. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members, because Defendant failed to implement the data management and security measures that are mandated by industry standards.

163. Defendant failed to secure the PII of Plaintiffs and Class Members and, therefore, did not provide full compensation for the benefit Plaintiffs and Class Members provided.

164. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

165. If Plaintiffs and Class Members knew that Defendant would not secure their PII using adequate security, they would not have made purchases or developed a financial relationship with Defendant.

166. Plaintiffs and Class Members have no adequate remedy at law.

167. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of customers and former customers in its continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (ix) the diminished value of Defendant's goods and services they received.

168. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including,

but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

169. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that it unjustly received from Plaintiffs and Class Members. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendant's goods and services.

COUNT V
Violation of the California Unfair Competition Law,
Cal. Bus. & Prof. Code § 17200, *et seq*. – Unlawful Business Practices
(On Behalf of the California Subclass)

170. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 113.

171. Defendant has violated Cal. Bus. and Prof. Code § 17200, *et seq*., by engaging in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in Cal. Bus. Prof. Code § 17200 with respect to the services provided to the California Class.

172. Defendant engaged in unlawful acts and practices with respect to the services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiffs' and California Subclass Members' PII with knowledge that the information would not be adequately protected; and by storing Plaintiffs' and California Subclass Members' PII in an unsecure environment in violation of California's data breach statute, Cal. Civ. Code § 1798.81.5, which requires Defendant to take reasonable methods of safeguarding the PII of Plaintiffs and the California Subclass Members.

173. In addition, Defendant engaged in unlawful acts and practices by failing to disclose the Data Breach to California Subclass Members in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82.

174. As a direct and proximate result of Defendant's unlawful practices and acts, Plaintiffs and the California Subclass Members were injured and lost money or property, including but not limited to the price received by Defendant for the services, the loss of California Subclass Members' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

175. Defendant knew or should have known that Defendant's computer systems and data security practices were inadequate to safeguard California Subclass Members' PII and that the risk of a data breach or theft was highly likely, especially given Defendant's inability to adhere to basic encryption standards and data disposal methodologies. Defendant's actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the California Subclass.

176. California Subclass Members seek relief under Cal. Bus. & Prof. Code § 17200, *et seq.*, including, but not limited to, restitution to Plaintiffs and California Subclass Members of money or property that Defendant may have acquired by means of Defendant's unlawful, and unfair business practices, restitutionary disgorgement of all profits accruing to Defendant because of Defendant's unlawful and unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

COUNT VI
Violation of California's Unfair Competition Law,
Cal. Bus. & Prof. Code § 17200, *et seq*. – Unfair Business Practices
(On Behalf of the California Subclass)

177. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 113.

178. Defendant engaged in unfair acts and practices with respect to the services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiffs' and California Subclass Members' PII with knowledge that the information would not be adequately protected; by storing Plaintiffs' and California Subclass Members' PII in an unsecure electronic environment; and by failing to properly dispose of equipment containing sensitive PII. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and California Subclass Members. They were likely to deceive the public into believing their PII was securely stored, when it was not. The harm these practices caused to Plaintiffs and the California Subclass Members outweighed their utility, if any.

179. Defendant engaged in unfair acts and practices with respect to the provision of services by failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect California Subclass Members' PII from further unauthorized disclosure, release, data breaches, and theft. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and California Subclass Members. They were likely to deceive the public into believing their PII was securely stored, when it was not. The harm these practices caused to Plaintiffs and the California Subclass Members outweighed their utility, if any.

180. As a direct and proximate result of Defendant's acts of unfair practices, Plaintiffs and the California Subclass Members were injured and lost money or property, including but not limited to the price received by Defendant for the services, the loss of California Subclass Members' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

181. Defendant knew or should have known that Defendant's computer systems and data security practices were inadequate to safeguard California Subclass Members' PII and that the risk of a data breach or theft was highly likely, including Defendant's failure to properly encrypt and dispose of equipment containing sensitive PII. Defendant's actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the California Subclass.

182. California Subclass Members seek relief under Cal. Bus. & Prof. Code § 17200, *et seq*., including, but not limited to, restitution to Plaintiffs and California Subclass Members of money or property that the Defendant may have acquired by means of Defendant's unfair business practices, restitutionary disgorgement of all profits accruing to Defendant because of Defendant's unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all Class Members, requests judgment against the Defendant and that the Court grant the following:

A. For an Order certifying the Nationwide Class and California Subclass as defined herein, and appointing Plaintiffs and their Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct

complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and the Class Members' PII, and from refusing to issue prompt, complete, any accurate disclosures to the Plaintiffs and Class members;

C. For equitable relief compelling Defendant to use appropriate cyber security methods and policies with respect to PII collection, storage, protection, and disposal, and to disclose with specificity to Plaintiffs and Class Members the type of PII compromised;

D. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of punitive damages;

F. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

G. For prejudgment interest on all amounts awarded; and

H. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

Date: July 29, 2020

Respectfully Submitted,

/s/ *Amanda Peterson*
AMANDA PETERSON (AP1797)
MORGAN & MORGAN
90 Broad Street, Suite 1011
New York, NY 10004
(212) 564-4568
apeterson@ForThePeople.com

JOHN A. YANCHUNIS
(*Pro Hac Vice application forthcoming*)
RYAN J. MCGEE
(*Pro Hac Vice application forthcoming*)
MORGAN & MORGAN
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602

(813) 223-5505
jyanchunis@ForThePeople.com
rmcgee@ForThePeople.com

M. ANDERSON BERRY
(*Pro Hac Vice application forthcoming*)
LESLIE GUILLON
(*Pro Hac Vice application forthcoming*)
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
(916) 777-7777
aberry@justice4you.com
lguillon@justice4you.com

WILLIAM 'BILLY' PEERCE HOWARD
(*Pro Hac Vice application forthcoming*)
HEATHER H. JONES
(*Pro Hac Vice application forthcoming*)
THE CONSUMER PROTECTION FIRM
4030 Henderson Boulevard
Tampa, FL 33629
(813) 500-1500
Billy@TheConsumerProtectionFirm.com
Heather@TheConsumerProtectionFirm.com